Amendment to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

~~Listing~~ of Claims:

1. (canceled)

2. (currently amended) A method of implementing an elliptic curve ~~cryptography~~ cryptographic operation in an apparatus implementing an elliptic curve cryptography ~~according to claim 1,~~in a finite field of characteristic 2 (or an extension field of "2"), in which said elliptic curve is given by $y^2 + xy = ax^2 + b$ and in which x and y are variables in an x-y coordinate system, a and b are parameters, addition of points P1 (x1, y1) and P2 (x2, y2) on said elliptic curve composed of points defined by individual coordinate components is presumed to be represented by P3 (x3, y3) with subtraction of said points P1 (x1, y1) and P2 (x2, y2) being presumed to be represented by P4 (x4, y4), ~~further~~ comprising the steps of:

inputting the coordinate component x1;

transforming said inputted coordinate component x1 into x- coordinates and z-coordinates $[X_1, Z_1]$ of a projective space where z is a variable of a projective space where z is a variable in the z-coordinate;

storing said coordinates $[X_1, Z_1]$ of said projective space;

transforming said coordinate component x2 into coordinates $[X_2, Z_2]$ of said projective space;

storing said projective coordinates $[X_2, Z_2]$;

transforming said coordinate component x4 into coordinates $[X_4, Z_4]$ of said projective space;

storing said coordinates $[X_4, Z_4]$;

determining projective coordinates $[X_3, Z_3]$ from said stored projective coordinates $[X_1, Z_1]$, $[X_2, Z_2]$ and $[X_4, Z_4]$;

transforming said projective coordinates $[X_3, Z_3]$ into said coordinate component x3; and

outputting said coordinate component x3,

whereby scalar multiplication of said point P1 (x1, y1) is determined;

generating a random number k;

storing said generated random number k;

transforming the x-coordinates into projective coordinates to thereby derive projective coordinates $[k^2x, k]$ through arithmetic operation of individual coordinate components of said projective space and said stored random number k.

3. (currently amended) A method of implementing an elliptic curve ~~cryptography~~ cryptographic operation in an apparatus implementing an elliptic curve cryptography in a finite field of characteristic 2 (or an extension field of "2"), in which said elliptic curve is given by $y^2 + xy = ax^2 + b$ and in which x and y are variables in

an x-y coordinate system, a and b are parameters, addition of points P1 (x1, y1) and P2 (x2, y2) on said elliptic curve composed of points defined by individual coordinate components is presumed to be represented by P3 (x3, y3) with subtraction of said points P1 (x1, y1) and P2 (x2, y2) being presumed to be represented by P4 (x4, y4), comprising the steps of:

inputting the coordinate component x1;

transforming said inputted coordinate component x1 into x- and z-coordinates $[X_1, Z_1]$ of a projective space where z is a variable of a projective space where z is a variable in the z-coordinate;

A12

storing said coordinates $[X_1, Z_1]$ of said projective space;

transforming said coordinate component x2 into coordinates $[X_2, Z_2]$ of said projective space;

storing said projective coordinates $[X_2, Z_2]$;

transforming said coordinate component x4 into coordinates $[X_4, Z_4]$ of said projective space;

storing said coordinates $[X_4, Z_4]$;

determining projective coordinates $[X_3, Z_3]$ from said stored projective coordinates $[X_1, Z_1]$, $[X_2, Z_2]$ and $[X_4, Z_4]$;

transforming said projective coordinates $[X_3, Z_3]$ into said coordinate component x3; and

outputting said coordinate component x3,

whereby scalar multiplication of said point P1 (x1, y1) is determined;~~according to claim 1,~~

~~further comprising the steps of:~~

generating a random number k;

storing said generated random number k;

transforming the x-_coordinates into projective coordinates to thereby derive projective coordinates [kx, k] through arithmetic operation of individual coordinate components of said projective space and said stored random number k.

A12

4. - 5. (canceled)

6. (currently amended) An apparatus implementing an elliptic curve ~~cryptography~~ cryptographic operation in a finite field of characteristic 2 (or an extension field of "2"), in which x and y are variables in an x-y coordinate system, a and b are parameters, said elliptic curve is given by $y^2 + xy = x^3 + ax^2 + b$, comprising:

random number generating means for generating a random number k;

projective coordinate transformation means receiving as inputs thereto coordinate x0 of said finite field of characteristic 2 and said random number k, to thereby transform said coordinate x0 into projective coordinates [kx0, k] = [X_1, Z_1];

doubling arithmetic means for arithmetically determining a double point from said projective coordinates [X_1, Z_1];

addition arithmetic means for determining an addition point from said projective coordinate $[X_1, Z_1]$ where Z is a variable in the z-coordinate to thereby output said addition point; and

scalar multiplication means receiving information from said projective coordinate transformation means, said doubling arithmetic means and said addition arithmetic means to thereby perform scalar multiplication of the coordinate component x0.

7. (canceled)

A12

8. (currently amended) A recording medium storing a program for implementing an elliptic curve ~~cryptography~~ cryptographic operation, said recording medium being in an apparatus implementing an elliptic curve cryptography ~~according to claim 7,~~

~~said program further comprising the statements of:~~in a finite field of characteristic 2 (or an extension field of "2"), in which said elliptic curve is given by $y^2 + xy = x^3 + ax^2 + b$, in which x and y are variables in an x-y coordinate system, a and b are parameters, addition of points P1 (x1, y1) and P2 (x2, y2) on said elliptic curve composed of points defined by individual coordinate components is presumed to be represented by P3 (x3, y3) with subtraction of points P1 (x1, y1) and P2 (x2, y2) being presumed to be represented by P4, (x4, y4), said program when executed causing the apparatus to perform:

inputting an coordinate component x1;

transforming said inputted coordinate component x1 into x- and z-coordinates $[X_1, Z_1]$ in a projective space;

storing said coordinates $[X_2, Z_2]$ of said projective space;

transforming said coordinate component x2 into coordinates $[X_2, Z_2]$ of said projective space;

storing said projective coordinate $[X_1, Z_1]$ where z is a variable in the z-coordinate;

A13

transforming said coordinate component x4 into coordinates $[X_4, Z_4]$ of said projective space;

storing said projective coordinates $[X_4, Z_4]$;

determining projective coordinates $[X_3, Z_3]$ from said stored projective coordinates $[X_1, Z_1]$, $[X_2, Z_2]$ and $[X_4, Z_4]$;

transforming said projective coordinates $[X_3, Z_3]$ into said coordinate component x3; and

outputting said coordinate component x3,

whereby scalar multiplication of said point P1 (x1, y1) is determined;

generating a random number k;

storing said generated random number k;

transforming the x-coordinates into projective coordinates to thereby derive projective coordinates $[k^2x, k]$ through arithmetic operation of individual coordinate components of said projective space and said stored random number k.

9. (currently amended) A recording medium storing a program for implementing an elliptic curve ~~cryptography~~ cryptographic operation, said recording medium being in an apparatus implementing an elliptic curve cryptography in a finite field of characteristic 2 (or an extension field of "2"), in which said elliptic curve is given by $y^2 + xy = x^3 + ax^2 + b$, in which x and y are variables in an x-y coordinate system, a and b are parameters, addition of points P1 (x1, y1) and P2 (x2, y2) on said elliptic curve composed of points defined by individual coordinate components is presumed to be represented by P3 (x3, y3) with subtraction of points P1 (x1, y1) and P2 (x2, y2) being presumed to be represented by P4, (x4, y4), said program when executed causing the apparatus to perform:

inputting an coordinate component x1;

transforming said inputted coordinate component x1 into x- and z-coordinates $[X_1, Z_1]$ in a projective space;

storing said coordinates $[X_2, Z_2]$ of said projective space;

transforming said coordinate component x2 into coordinates $[X_2, Z_2]$ of said projective space;

storing said projective coordinate $[X_1, Z_1]$ where z is a variable in the z-coordinate;

transforming said coordinate component x4 into coordinates $[X_4, Z_4]$ of said projective space;

storing said projective coordinates $[X_4, Z_4]$;

determining projective coordinates $[X_3, Z_3]$ from said stored projective coordinates $[X_1, Z_1]$, $[X_2, Z_2]$ and $[X_4, Z_4]$;

transforming said projective coordinates $[X_3, Z_3]$ into said coordinate component x3; and

outputting said coordinate component x3,

whereby scalar multiplication of said point P1 (x1, y1) is determined;~~according to claim 7,~~

A12

~~said program further comprising the statements of:~~

generating a random number k;

storing said generated random number k;

transforming the x-_coordinates into projective coordinates to thereby derive projective coordinates [kx, k] through arithmetic operation of individual coordinate components of said projective space and said stored random number k.

10. - 12. (canceled)